

Notice of Allowability

Application No.

10/058,442

Examiner

Robert W. Wilson

Applicant(s)

DONAGHEY, ROBERT J.

Art Unit

2616

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 5/11/07.
2. ☒ The allowed claim(s) is/are 11-12, 14, 16-17, 19-24, 32-33, 36, & 39-41 (Re#1-17).
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
- * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|--|---|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____ |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____ | 7. <input type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____ |

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Edward Gordon on 7/17/07.

The application has been amended as follows:

Delete the following from Pg 1 Para [01] of the specification:

"Moreover, this application relates to U.S. Patent Serial No.: _____ (Docket No. 01-04003A), and U.S. Patent Application Serial No. _____ (Docket No. 01-4003C), filed concurrently herewith are hereby incorporated herein by reference in their entireties"

Replace with the following to Pg 1 Para[01] of the specification in place of the deleted material:

Moreover, this application relates to U.S. Patent Serial No.: 10/058,487 (Docket No. 01-04003A), and U.S. Patent Application Serial No.10/058,512 (Docket No. 01-4003C), filed concurrently herewith are hereby incorporated herein by reference in their entireties"

Allowable Subject Matter

2. Claims 11-12, 14, 16-17, 19-24, 32-33, 36, 39-41 are allowed.

The following is an Examiner's statement of reasons for allowance: Claims 11-12, 14, 16-17, 19-24, 32-33, 36, 39-41 are considered allowable since when reading the claims in light of the specification, none of the references of record alone or in combination disclose or suggest the combination of limitations specified in the independent claims including:

"associated at least one annotation with the at least one feature, the at least one annotation including an annotation identifying the first filter technique and create at least one model

Art Unit: 2616

reflecting a behavior of the first user based on the features associated with the group of packets” as claimed in claim 11 & claim 21.

“means for comparing the features associated with a group of packets with features of each of the at least one identified model, means for generating a closeness score for each of the at least one identified model based on the comparing, means for determining whether the closeness score for each of the at least one identified model equals or exceeds a threshold; means for identifying the group of packets as a normal group when the closeness score of at least one of the identified models equals or exceeds the threshold, means for allowing groups of packets classified as normal group to pass on toward their destination, and means for filtering groups of packets classified as attack groups using filtering technique”, as specified in claim 32.

“compare the features associated with a group of packets with features of each of the at least one identified model, generate a closeness score for each of the at least one identified model based on the comparing, determine whether the closeness score for each of the at least one identified model equals or exceeds a threshold. Identify the group of packets as a normal group when the closeness score of at least one of the identified models equals or exceeds the threshold, allow groups classified as normal groups to pass on toward their destination and filter groups classified as attack groups using the first filtering technique” as claimed in claim 33.

“comparing the features associated with a packet group with features of each of the at least one HMMs, generating a closeness score for each of the at least one HMMs based on the comparing, comparing the closeness score to a threshold, identifying the packet group as a normal group when at least one of the closeness scores equals or exceeds the threshold and allowing the groups of packet identified as normal group to pass on toward their destination and filtering packet groups classified as attack group using the first filter technique as claimed in claim 41.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Robert W. Wilson whose telephone number is 571/272-3075.

The examiner can normally be reached on M-F (8:00-4:30).

Art Unit: 2616

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on 571/272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Robert W Wilson
Examiner
Art Unit 2616

RWW
7/18/07

EDAN ORGAD
PRIMARY PATENT EXAMINER

